ICH/Secom
cln ADP

DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-070

11 Marcn 1986

MEMORANDUM FOR: SECOM Members

STAT

FROM: [redacted]
Chairman

SUBJECT: Personal Computer Guidelines

Attached is the final draft of the personal computer security guidelines which has taken into account the comments of the SECOM members, the Computer Security Subcommittee members and the Information Handling Committee Staff. Please be prepared to discuss it at the SECOM on 19 March so that it can be finally approved.

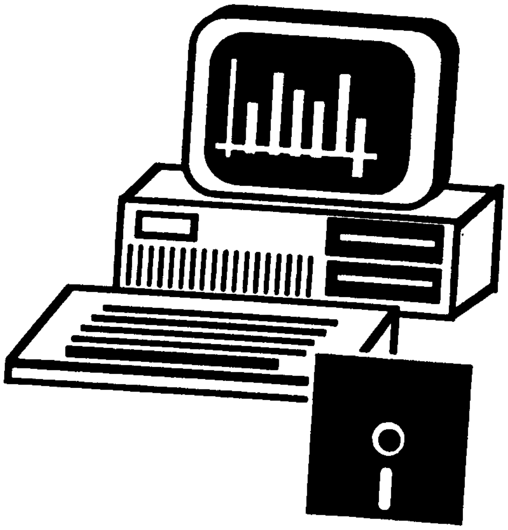
STAT

[redacted]

Attachment: a/s

Processing INTELLIGENCE INFORMATION On Personal Computer Systems...

[redacted]



- A User's Guide -

Foreword

This booklet provides security guidance for users of personal computer systems (PCs) for the processing of Intelligence Information. It is intended to help PC users comply with *DCID 1/16: Security Policy on Intelligence Information in Automated Systems and Networks.*

Requirements are described for:

Acquisition and Maintenance
Physical and Operational Control
Multiple User Systems
Networked PCs
Equipment and Media Disposal

The requirements described are basic controls. Individual agencies may establish additional requirements, if deemed appropriate.

Contact your Information System Security Officer (ISSO) for specific guidance and assistance.

Your ISSO is:

Telephone:

Personal Computers and Intelligence Information

The Personal Computer (PC) has given us a powerful new tool for handling information efficiently and accurately. In many ways, it has changed the way in which we store, process, transmit, and even think about Intelligence Information.

However, increased PC use also increases the risk that such information may be accidentally or intentionally compromised, modified or destroyed. Information in a PC often is less visible, more highly concentrated, and more easily manipulated than the same information in hardcopy form. Therefore, we need to take special steps to protect PC-based information.

[redacted]

The PC may be changing the way we process information, but security requirements for the protection of Intelligence Information haven't changed.

So, before you begin using a PC to handle such information, you need to think about ...

THINK ABOUT . . .

ACQUISITION AND MAINTENANCE PROCEDURES

Because of the highly technical nature of PC equipment, steps must be taken to ensure that the use of PC systems to process Intelligence Information neither results in the inadvertent disclosure of information nor provides an adversary with the ability to intercept such information. It is important, therefore, that PC equipment and its use be controlled throughout its serviceable life cycle.

Accountability . . .

The Information System Security Officer (ISSO), whose name and phone number are listed on the inside front cover of this booklet, is assigned formal security responsibility for your PC System. However, it is **YOUR** responsibility to assure that proper security procedures are followed during its use.

Acquisition . . .

All PC equipment and software to be used for processing Intelligence Information must be acquired for such use through your agency's approved channels.

Approval for Use . . .

The ISSO must ensure that each PC System is approved for a given operational environment and use. If the PC system is removed from that environment, modified in any way, or put to any different use, it must be re-approved before being used again to process Intelligence Information.

Personally-Owned Equipment ...

No personally-owned equipment, software, or media may be used to process Intelligence Information. If such items are brought into an operational environment where Intelligence Information is processed, they may NOT be removed without the ISSO's approval.

TEMPEST Controls . . .

A PC system being used to process Intelligence Information must be TEMPEST-approved for the specific operational environment and location. Such approval should be clearly indicated on each separate PC system component (e.g, disk drive, display unit, printer, etc). Any change to the approved configuration, including either internal components (e.g., memory boards) or external devices (e.g., printer or cabling), or re-location to another operational environment requires re-approval. You must not remove equipment covers or attempt to perform any maintenance.

Maintenance . . .

Maintenance activity may affect the integrity of existing protection measures or permit the introduction of security exposures into a system. Particular care must be taken whenever maintenance must be performed on PC equipment. Maintenance must be performed only by properly cleared persons. Equipment (including components and software) may not be removed from the operational environment without approval of the ISSO. Equipment must be re-approved for use upon return from maintenance.

THINK ABOUT . . .

PHYSICAL AND OPERATIONAL CONTROLS

The PC performs the functions of several traditional office devices -- a typewriter, calculator, communications device, and file cabinet -- for handling Intelligence Information.

You should secure PC systems in the same manner as you would other office devices and storage containers ... Lock them up, control personnel access, and ensure proper disposal and accountability of any classified material.

Basic physical security controls will limit access to the area and prevent placement of monitoring or recording devices. Operational security procedures will protect the Intelligence Information against unauthorized access.

Personnel Access . . .

All persons permitted to use the equipment, view information displayed by the system, or access any associated classified materials (including diskettes and printed material) must have appropriate clearances and the need-to-know.

A sign or other indication should be displayed when Intelligence Information processing is taking place. The back panel of this booklet can be folded out to form a "tent card" for this purpose.

Classification Markings . . .

All classified material, media, and equipment must be clearly labeled with the highest classification level and any compartmentation controls associated with the information contained therein. Printouts, diskettes, and other storage media or devices should be considered classified at the level of the PC system and the Intelligence Information being processed. Such material must be handled, transmitted, and stored as appropriate for that level of Intelligence Information.

Printouts must be reviewed manually (even if the PC initially prints the classification markings) and then marked with the appropriate classification.

Each diskette (including system, utilities, and program disks) must have an external label clearly indicating the highest classification level of any system on which it has been used. (Contact your ISSO for required labels.)

You, as a user, may **NEVER** reduce the classification level of diskettes.

Caution: Purchased software diskettes must never be returned to the vendor (e.g. for version upgrades) if such diskettes have ever been used in a classified PC system.

Unclassified diskettes should be labeled as such. Diskettes must be re-labeled with the appropriate classification when used in a PC System containing Intelligence Information.

Creating Downgraded Extracts or Files . . .

Extreme care must be taken when producing downgraded extracts from classified materials because of the possibility of higher classified information being included in the resulting extract. This could occur accidentally or through the use of modified or corrupted software. It is best, therefore, only to use a PC system which does not contain any information classified higher than the level of the Intelligence Information you currently wish to process.

An acceptable method for producing (extracting) a file of lower classification than that of the PC system or the magnetic media on which it resides is first to produce a hardcopy version (i.e., printout) of the file. After **human review**, the information must be transcribed (from the hardcopy) to appropriately classified media on another PC system which is operating at the lower classification level. You may wish to see your ISSO for additional guidance.

Transmittal...

Before you transfer custody of a diskette, removable hard disk, or any other such media, you must be certain that the recipient has the necessary clearances and need-to-know for **ALL** the information contained therein. **(Caution: Normal file deletion procedures do not remove the actual data in a disk file.)** You must also use appropriate receipting procedures to record the transfer. **Remember, you are responsible for protecting Intelligence Information!**

Clearing the PC System . . .

A PC system becomes classified to the level of any classified Intelligence Information that has been entered into or produced by the system. It will remain classified at the highest level of the Intelligence Information until and unless the PC System can be appropriately cleared and certified as Unclassified. Therefore, upon completion of processing, the following must be done:

- Diskettes and printer ribbons should be removed and properly secured. Cardboard inserts should be placed in diskette drives to provide evidence that diskettes have been removed.

- Classified data should be cleared from all system memory devices. See your ISSO for procedures appropriate for your specific PC system.

If classified data CANNOT be cleared from all system components (e.g., non-removable hard disk or other non-volatile storage) the PC system remains, by definition, classified material. It must, therefore, be labeled accordingly and secured in accordance with the requirements for any other material of the same classification level.

Regardless of the use of any clearing process, a PC System which has ever been used to process Intelligence Information may be never removed from its operational environment without the ISSO's approval.

Use A Checklist . . .

Include specific PC security measures in the daily security checklist for your work area.

THINK ABOUT . . .

MULTIPLE USERS

A PC system (unless it has been cleared in accordance with the previous procedures) may not be used by multiple users (either concurrent or sequential) unless each user has clearances and need-to-know for ALL Intelligence Information on the system. This equates to operating in the DEDICATED or SYSTEM HIGH modes of operation. **CAUTION: There is a degree of risk in SYSTEM HIGH mode operation, since a PC cannot provide the system controls and audit trails normally required for such operation.** A PC system may NOT be operated in COMPARTMENTED mode unless specifically designed and approved for such use.

THINK ABOUT . . .

NETWORKED PC'S

An important characteristic of a PC which is connected to any type of data communications facility or network is that data can be transmitted to and from the PC memory or storage devices. It may also be possible for the PC or its files to be manipulated directly by a remote user or process. This can take place rapidly and without the knowledge or control of the PC user. Therefore, certain precautions are required.

A PC may not be connected to any network unless it has been certified to be in compliance with all security requirements of the network and host computer system. Such a connection must not violate the integrity of any COMSEC measures in effect on the network.

A PC may not be connected to a network or system of lower classification than that of the PC itself. Once connected, the PC and all storage devices and media of the system assume the highest classification of the network or host system.

A PC normally cannot provide adequate user authentication or access controls for remote users. Therefore, PCs used for processing Intelligence Information may not be set up for dial-in access unless specifically designed and approved for such use.

Logon passwords and other such information which permit access to a network or host system should not be stored on a user's PC.

THINK ABOUT . . .

EQUIPMENT AND MEDIA DISPOSAL

PC equipment which has been used for Intelligence Information processing shall not be released from agency control until the equipment is certified by the ISSO as Unclassified. Disposal of equipment must be only through approved agency control channels.

Unusable or inoperative media (including self-contained storage devices such as fixed disk units) must be disposed of using methods approved by the ISSO.

Printouts, ribbons, diskettes, and other such items used in Intelligence Information processing must be destroyed as Classified waste.

DO YOUR PART!

Personal computers provide us with very important benefits in terms of efficiency, availability and reliability in handling Intelligence Information. However, these benefits are negated if the security of such information is jeopardized in the process.

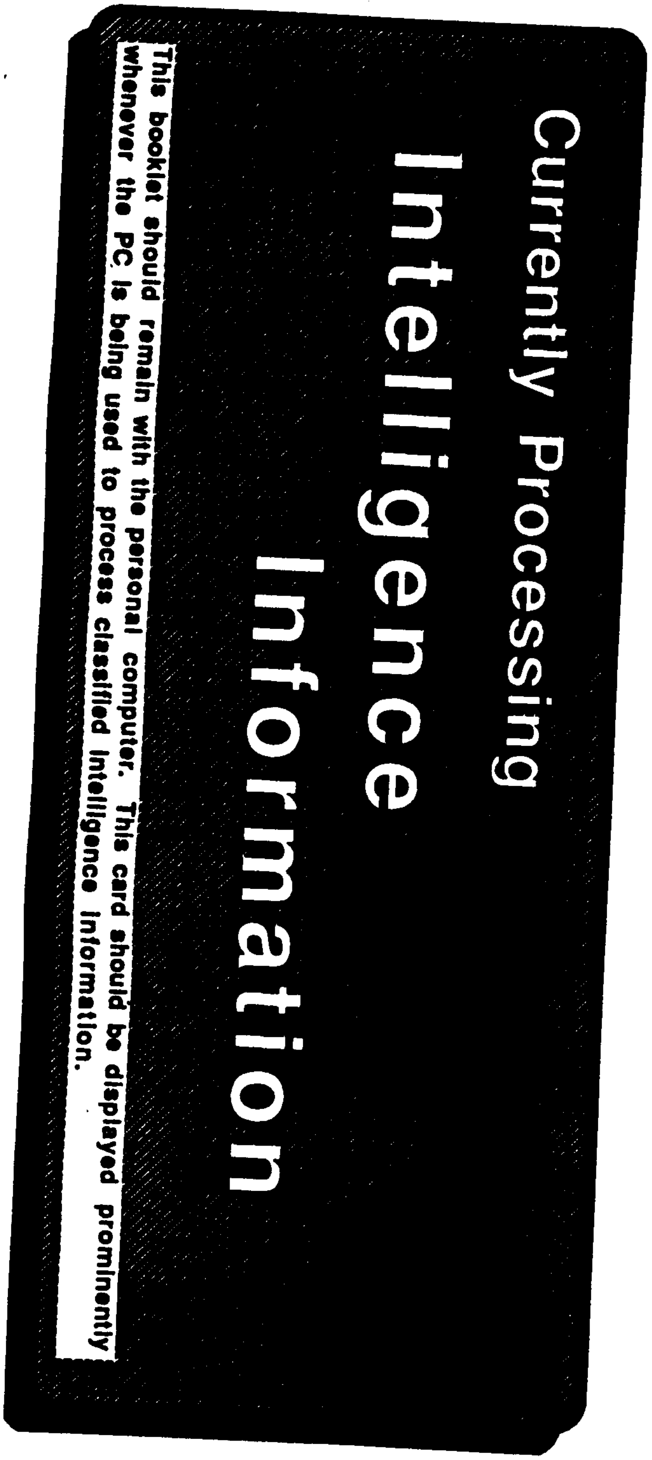
Therefore, **YOU** must be aware of the potential risks and **YOU** must assume personal responsibility for the protection of Intelligence Information when using PC systems.

You should report all PC-related security incidents to your ISSO.

[redacted]

For Additional Guidance ...

This booklet provides you with basic security guidance for the processing of Intelligence Information on personal computers. More detailed guidance may apply to various specific situations, and your agency may have additional or more specific policies or procedures. You should contact your Information System Security Officer (ISSO) for additional guidance, as well as for clarification and assistance in implementing the guidance provided herein.



Currently Processing

Intelligence

Information

This booklet should remain with the personal computer. This card should be displayed prominently whenever the PC is being used to process classified Intelligence Information.

The Intelligence Community Staff is responsible for specific policy on the protection of Intelligence Information processed on PC Systems.

For more information contact:
DCI
Security Committee
Computer Security Subcommittee
Intelligence Community Staff
Washington, DC 20505